

REMARKS

[0001] Applicant respectfully requests reconsideration and allowance of all of the claims of the application. Claims 1-27 are presently pending. Claims amended herein are 1, 11-15, 19, 36, and 27.

Statement of Substance of Interview

[0002] The Examiner graciously talked with me—the undersigned representative for the Applicant—on July 22, 2008. Applicant greatly appreciates the Examiner's willingness to talk. Such willingness is invaluable to both of us in our common goal of an expedited prosecution of this patent application.

[0003] During the interview, it was established that the Office Action that was mailed on May 28, 2008 was, in fact, not intended to be a final Office Action. The Examiner indicated that he would remedy this mistake and that the Applicant could respond as though the Office Action was not final. Further, I discussed how the claims differed from the prior art of record as well as reasons why the recited claims currently recite allowable subject matter. Without conceding the propriety of the rejections and in the interest of expediting prosecution, I also proposed several possible clarifying amendments.

[0004] The Examiner was receptive to the proposals, specifically the clarification regarding allowable subject matter for claims 1, 13-15, 26 and 27. However, the Examiner indicated that he would need to review the language more carefully, and requested that the proposed amendments be presented in writing.

[0005] Applicant herein amends the claims in the manner discussed during the interview. Accordingly, Applicant submits that the pending claims are allowable over the cited art of record for at least the reasons discussed during the interview.

Formal Request for an Interview

[0006] If the Examiner's reply to this communication is anything other than allowance of all pending claims, then I formally request an interview with the Examiner. I encourage the Examiner to call me—the undersigned representative for the Applicant—so that we can talk about this matter so as to resolve any outstanding issues quickly and efficiently over the phone.

[0007] Please contact me to schedule a date and time for a telephone interview that is most convenient for both of us. While email works great for me, I welcome your call as well. My contact information may be found on the last page of this response.

Allowable Subject Matter

[0008] Applicant would like to thank the Examiner for indicating allowable subject matter for claims 4 and 8-14. These claims have not been amended other than for clarification for §101 reasons herein, and therefore remain allowable.

Claim Amendments

[0009] Without conceding the propriety of the rejections herein and in the interest of expediting prosecution, Applicant amends claims 1, 11-15, 26 and 27 herein. Applicant amends claims to clarify claimed features. Such amendments are made to expedite prosecution and more quickly identify allowable subject

matter. Such amendments are merely intended to clarify the claimed features, and should not be construed as further limiting the claimed invention in response to the cited references.

Substantive Matters

Claim Rejections under § 112 1ST ¶

[0010] Claims 20 is rejected under 35 U.S.C. § 112, 1st ¶. Applicant respectfully traverses this rejection. Furthermore, in light of the amendments presented previously, Applicant submits that these rejections are moot and reasons for such are presented below. Accordingly, Applicant asks the Examiner to withdraw these rejections.

[0011] Claim 20 recites generating the first pseudo-random value from a previous chaos-based pseudo-random value. Such a recitation is supported, for example, by paragraph 54 of the present application. The method of generating a chaos-based pseudo-random value “could be easily repeated” so that the chaos-based pseudo-random value of a generator can be used by other “generators of sequences of pseudo-random numbers” (paragraph 54). The first pseudo-random value recited in claim 15 is generated with a chaotic map, and therefore, is a chaos-based pseudo-random value. As the present application clearly states (in paragraph 54), this method can easily be repeated so that the chaos-based pseudo-random value recited in claim 15 is generated from a similar chaos-based pseudo-random value (as recited in claim 20). Therefore, claim 20 is clearly supported by the specification.

[0012] Based on the text of the rejection in the Office Action, it appears that the Examiner is under the impression that the recitation of “before the first-chaos-based pseudo-random value” remains part of claim 20. Applicant specifically points out that claim 20 was amended in the most recent Request for Continued

Examination. Thus, with regard to the § 112, 1st ¶ rejection, Applicant respectfully traverses as the argument presented is moot.

Claim Rejections under § 101

[0013] Claims 1-10 and 13-27 are rejected under 35 U.S.C. § 101. Applicant respectfully traverses this rejection. Furthermore, in light of the amendments presented herein, Applicant respectfully submits that these claims comply with the patentability requirements of §101 and that the §101 rejections should be withdrawn. Applicant further asserts that these claims are allowable. Accordingly, Applicant asks the Examiner to withdraw these rejections.

[0014] In specific, claims 1 and 15 have been amended to recite “storing said chaos-based pseudo-random sequence in a circuit” as suggested by the Examiner during the Examiner Interview of July 22, 2008. This recitation certainly provides an enumerated statutory category (the circuit means is a device (*i.e.*, a machine) and when storing the sequence therein, a physical transformation of stored energy is realized.

[0015] Further, claims 13, 14, 26, and 27 have been amended to recite “operable to be used in an encryption application” as suggested by the Examiner during the Examiner Interview of July 22, 2008. This recitation certainly provides an enumerated statutory category (the circuit/memory is a device (*i.e.*, a machine) and accomplishes a practical application as encryption technology ensures the secure transmission of sensitive data over networks.

[0016] If the Examiner maintains the rejection of these claims, then Applicant requests additional guidance as to what is necessary to overcome the rejection.

Claim Rejections under § 102

[0017] The Examiner rejects claims 1-3, 5-7, and 15-27 under § 102. For the reasons set forth below, the Examiner has not shown that the cited references anticipate the rejected claims.

[0018] Accordingly, Applicant respectfully requests that the § 102 rejections be withdrawn and the case be passed along to issuance.

[0019] The Examiner's rejections are based upon the following references:

- **Butler 6,678,707:** *Butler* US Patent No. 6,678,707 (issued January 13, 2004); and
- **Smeets 6,253,236:** *Smeets* US Patent No. 6,253,236 (issued November 2, 2007).

Anticipation Rejections

[0020] Applicant submits that the anticipation rejections are not valid because, for each rejected claim, no single reference discloses each and every element of that rejected claim.¹ Furthermore, the elements disclosed in the single reference are not arranged in the manner recited by each rejected claim.²

Based upon Butler 6,678,707

[0021] The Examiner rejects claims 1-3, 5-7, and 15-27 under 35 U.S.C. § 102(e) as being anticipated by Butler 6,678,707. Applicant respectfully traverses the rejection of these claims. Based on the reasons given below, Applicant asks the Examiner to withdraw the rejection of these claims.

Independent Claim 1

[0022] Applicant submits that Butler 6,678,707 does not anticipate this claim because it does not disclose the following elements as recited in this claim:

- “defining a function ($H(x)$) on a first interval ($x \in [0, q]$) whose inverse has a plurality of branches;”
- “generating numbers of said pseudo-random sequence (x_n);”

¹ “A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference.” *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987); also see MPEP §2131.

² See *In re Bond*, 910 F.2d 831, 15 USPQ2d 1566 (Fed. Cir. 1990).

- “calculating numbers of a chaos-based pseudo-random sequence (X_n) by applying said function ($H(x)$) to corresponding integer numbers of said pseudo-random sequence (x_n).”]

[0023] The Examiner indicates (Action, p. 4) the following with regard to this claim:

As per claims 1, 15, 16, 18, 19, 21, 26 and 27, Butler discloses in figure 8 a generation of a chaos-based pseudo-random sequence in an encryption application, including defining a chaotic map (402-412) for generating a pseudo-random sequence of integer numbers in a certain interval, choosing a seed (the initial states) for the pseudo-random sequence of integer numbers, and generating numbers of the pseudo-random sequence, defining a function (800) on the interval whose inverse has a plurality of branches and calculating numbers of a chaos-based pseudo-random sequence by applying the function to corresponding integer numbers of the pseudorandom sequence as claimed.

[0024] Claim 1 recites “generating numbers of a pseudo-random sequence and calculating numbers of a chaos-based pseudo-random sequence by applying a function to corresponding integer numbers of the pseudo-random sequence, where the inverse of the function has a plurality of branches[.]”

[0025] For example, referring to paragraphs 52-70 of the present application, a method includes generating numbers of a pseudo-random sequence x_n and calculating numbers of a chaos-based pseudo-random sequence X_n by applying a function $H(x)$ to corresponding integer numbers of the pseudo-random sequence x_n , where the inverse of the function $H(x)$ has a

plurality of branches. It should be noted that the generated sequence x_n is pseudo-random, and by definition is reconstructable from a seed (paragraph 11). This is only possible if the generated sequence is not random, but pseudo-random. It is important that the generated sequence be pseudo-random so that the sequence can be reconstructed for decrypting.

[0026] Butler 6,678,707, on the other hand, does not disclose generating numbers of a pseudo-random sequence and calculating numbers of a chaos-based pseudo-random sequence by applying a function to corresponding integer numbers of the pseudo-random sequence, where the inverse of the function has a plurality of branches. Quite differently, Butler 6,678,707 addresses the problem of generating truly random numbers (col. 4, lines 35-40). As a result, Butler 6,678,707 cannot be used in cryptographic codes in which the receiver of the data needs to reconstruct the random number sequence to decrypt the data because Butler 6,678,707 generates a sequence of truly random numbers that is unpredictable. Generating a truly random sequence of numbers that cannot be repeated (as taught in Butler 6,678,707) is not the same generating a pseudo-random sequence (as recited in claim 1 and supported in the application at col. 6, lines 6-9).

[0027] More specifically, Butler 6,678,707 discloses a means 800 that carries out a post-processing algorithm for eliminating all possible correlations/dependencies between successive random numbers generated by a MISR 402-412 (FIG. 8; col. 8, lines 5-27). The means 800 does not generate a sequence of chaos-based pseudo-random numbers by evolving from a given pseudo-random number used as a seed, but instead calculates only one truly

random number as a function of the current random number generated by the MISR 402-412 using a hash function or another function (col. 8, lines 16-27).

[0028] Consequently, Butler 6,678,707 does not disclose all of the elements and features of this claim. Accordingly, Applicant asks the Examiner to withdraw the rejection of this claim.

Dependent Claims 2-3 and 5-7

[0029] These claims ultimately depend upon independent claim 1. As discussed above, claim 1 is allowable. It is axiomatic that any dependent claim which depends from an allowable base claim is also allowable. Additionally, some or all of these claims may also be allowable for additional independent reasons.

Independent Claims 13, 14, 15, 26, and 27

[0030] Applicant submits that Butler 6,678,707 does not anticipate these claims because it does not disclose the following elements as recited in these claims:

- “a chaos-based pseudo-random value[.]”

[0031] The Examiner indicates (Action, p. 4) the following with regard to this claim:

As per claims 1,15,16,18,19,21,26 and 27, Butler discloses in figure 8 a generation of a chaos-based pseudo-random sequence in

an encryption application, including defining a chaotic map (402-412) for generating a pseudo-random sequence of integer numbers in a certain interval, choosing a seed (the initial states) for the pseudo-random sequence of integer numbers, and generating numbers of the pseudo-random sequence, defining a function (800) on the interval whose inverse has a plurality of branches and calculating numbers of a chaos-based pseudo-random sequence by applying the function to corresponding integer numbers of the pseudorandom sequence as claimed.

[0032] Each of these claims recites “a chaos-based pseudo-random value” as well as various additional recitations relevant to each claim focus. As discussed above, Butler 6,678,707 simply does not disclose generating numbers of a pseudo-random sequence and calculating numbers having a chaos-based pseudo-random value. Quite differently, Butler 6,678,707 addresses the problem of generating truly random numbers (col. 4, lines 35-40). As a result, Butler 6,678,707 cannot be used in cryptographic codes in which the receiver of the data needs to reconstruct the random number sequence to decrypt the data because Butler 6,678,707 generates a sequence of truly random numbers that is unpredictable. Generating a truly random sequence of numbers that cannot be repeated (as taught in Butler 6,678,707) is not the same generating a chaos-based pseudo-random values (as recited in these claims and supported in the application at col. 6, lines 6-9).

[0033] Consequently, Butler 6,678,707 does not disclose all of the elements and features of this claim. Accordingly, Applicant asks the Examiner to withdraw the rejection of this claim.

Dependent Claims 16-25

[0034] These claims ultimately depend upon independent claim 15. As discussed above, claim 15 is allowable. It is axiomatic that any dependent claim which depends from an allowable base claim is also allowable. Additionally, some or all of these claims may also be allowable for additional independent reasons.

Based upon Smeets 6,253,236

[0035] The Examiner rejects claims 1-3, 5-7, and 15-27 under 35 U.S.C. § 102(e) as being anticipated by Smeets 6,253,236. Applicant respectfully traverses the rejection of these claims. Based on the reasons given below, Applicant asks the Examiner to withdraw the rejection of these claims.

Independent Claim 1

[0036] Applicant submits that Smeets 6,253,236 does not anticipate this claim because it does not disclose the following elements as recited in this claim:

- “defining a chaotic map for generating a pseudo-random sequence of integer numbers (x_n) comprised in a certain interval $([0, q])$,”
- “defining a function ($H(x)$) on a first interval $(x[0, q])$ whose inverse has a plurality of branches;”
- “calculating numbers of a chaos-based pseudo-random sequence (X_n) by applying said function ($H(x)$) to corresponding integer numbers of said pseudo-random sequence $(x_n)[.]$ ”

[0037] The Examiner indicates (Action, p. 4-5) the following with regard to this claim:

As per claims 1, 15, 16, 18, 19, 21, 26 and 27, Smeets discloses in figure 2 a generation of a chaos-based pseudo-random sequence in an encryption application including defining a chaotic map (201) for generating a pseudo-random sequence of integer numbers in a certain interval, choosing a seed (the initial states) for the pseudo-random sequence of integer numbers, and generating numbers of the pseudo-random sequence (Z), defining a function $F(203)$ on the interval whose inverse has a plurality of branches and calculating numbers of a chaos-based pseudo random sequence by applying the function to corresponding integer numbers of the pseudo-random sequence as claimed.

[0038] Smeets 6,253,236 is directed to a device for use in a mobile phone for generating random noise for use in a communications between devices. However, the system and method employed by Smeets 6,253,236 is an example of the prior art in which the present application overcomes. In specific, it merely discusses the concept of pseudo random sequence generation but falls quite short of teaching the specific recitations of claim 1.

[0039] Claim 1 recites "defining a chaotic map for generating a pseudo-random sequence of integer numbers (x_n) comprised in a certain interval $([0, q])$." The Examiner contends that Smeets 6,253,236 teaches a chaotic map with reference to the sequence generators 201 of FIG 2. The sequence generators of Smeets 6,253,236 are merely conventional devices that are not based on a chaotic map. In fact, the words "chaotic map," "chaos-based" or even

the word “chaos” itself do not appear anywhere in Smeets 6,253,236. The Examiner cannot possibly contend that Smeets 6,253,236 teaches a chaotic map without being cognizant of the concept of chaos-based random number generation.

[0040] Further, claim 1 recites “calculating numbers of a chaos-based pseudo-random sequence (X_n) by applying said function ($H(x)$) to corresponding integer numbers of said pseudo-random sequence (x_n).]” Again, the words “chaotic map,” “chaos-based” or even the word “chaos” itself do not appear anywhere in Smeets 6,253,236. The Examiner cannot possibly contend that Smeets 6,253,236 teaches a chaotic map without being cognizant of the concept of chaos-based random number generation.

[0041] Further yet, claim 1 recites “defining a function ($H(x)$) on a first interval ($x[0, q]$) whose inverse has a plurality of branches[.]” There is simply no teaching anywhere in Smeets 6,253,236 that can possibly be construed as a function having an inverse with a plurality of branches. In fact, again, such words (“inverse” and “branches”) do not appear anywhere in Smeets 6,253,236.

[0042] Consequently, Smeets 6,253,236 clearly does not disclose all of the elements and features of this claim. Accordingly, Applicant asks the Examiner to withdraw the rejection of this claim.

Dependent Claims 2-3 and 5-7

[0043] These claims ultimately depend upon independent claim 1. As discussed above, claim 1 is allowable. It is axiomatic that any dependent claim

which depends from an allowable base claim is also allowable. Additionally, some or all of these claims may also be allowable for additional independent reasons.

Independent Claims 13, 14, 15, 26, and 27

[0044] Applicant submits that Smeets 6,253,236 does not anticipate these claims because it does not disclose the following elements as recited in these claims:

- “a chaos-based pseudo-random value[.]”

[0045] The Examiner indicates (Action, p. 4) the following with regard to this claim:

As per claims 1, 15, 16, 18, 19, 21, 26 and 27, Smeets discloses in figure 2 a generation of a chaos-based pseudo-random sequence in an encryption application including defining a chaotic map (20 l) for generating a pseudo-random sequence of integer numbers in a certain interval, choosing a seed (the initial states) for the pseudo-random sequence of integer numbers, and generating numbers of the pseudo-rand sequence (Z), defining a function F(203) on the interval whose inverse has a plurality of branches and calculating numbers of a chaos-based pseudo random sequence by applying the function to corresponding integer numbers of the pseudo-random sequence as claimed.

[0046] Each of these claims recites “a chaos-based pseudo-random value” as well as various additional recitations relevant to each claim focus. As

discussed above, Smeets 6,253,236 simply does not teach or, much less, is even cognizant of the concept of chaos-based pseudo-random value generation.

[0047] Consequently, Smeets 6,253,236 does not disclose all of the elements and features of this claim. Accordingly, Applicant asks the Examiner to withdraw the rejection of this claim.

Dependent Claims 16-25

[0048] These claims ultimately depend upon independent claim 15. As discussed above, claim 15 is allowable. It is axiomatic that any dependent claim which depends from an allowable base claim is also allowable. Additionally, some or all of these claims may also be allowable for additional independent reasons.

Conclusion

[0049] All pending claims are in condition for allowance. Applicant respectfully requests reconsideration and prompt issuance of the application. If any issues remain that prevent issuance of this application, the **Examiner is urged to contact me before issuing a subsequent Action.** Please call or email me at your convenience.

[0050] In the event additional fees are due as a result of this amendment, payment for those fees has been enclosed in the form of a check. Should further payment be required to cover such fees you are hereby authorized to charge such payment to Deposit Account No. 07-1897.

Respectfully Submitted,

Graybeal, Jackson, Haley, LLP
Representatives for Applicant

/Kevin D. Jablonski/
Kevin D. Jablonski (kevin@graybeal.com)
Registration No. 50,401

Dated: August 12, 2008

Telephone: (425) 455-5575
Facsimile: (425) 455-1046